ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The business at 45 Spring House Lane, Berryville, Virginia, is located in a residential home at the east end of Spring House Lane on the south side of the road. Spring House Lane intersects Hawthorne Lane. Hawthorne Lane, in turn, intersects Virginia Route 7 (also known as Harry Byrd Highway) approximately 3.7 miles east of U.S. route 340 (also known as Lord Fairfax Highway) in Berryville, Virginia.

45 Spring House Lane is described as a two-story, gray and stone home with white trim and a light black asphalt shingled roof. It has a wrap-around porch with a spindle rail and a dark brown wood front door with side panels. The door and both side panels have glass windows. A two-car garage is on the right side of the home when facing the property from Spring House Lane. The entrance to the garage faces to the right. There is also a brick chimney on the right side of the home. A dark brown, three-rail fence runs the length of the front and right sides of the property. The number "45" is displayed on the top rail of the fence behind the mailbox and newspaper box on a white sign; the numerals are black. The rear of the property contains a variety of full grown trees.


Spring House Ln
Spring House Ln
Spring House Ln
Spring House Ln
Spring House Ln
45 Spring House Lane


45

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND ANALYZED:

1. All records relating to violations of the Foreign Corrupt Practices Act ("FCPA") (15 U.S.C. §§ 78dd-1 et seq.), or conspiracy to commit violations of the FCPA (18 U.S.C. § 371), those violations involving ROBERT PRESTON KERN, the HUNTING CONSORTIUM and co-conspirators working with KERN and occurring after January 1, 2014, including:

   a. Identity of associates and possible co-conspirators and related identifying information;

   b. Any record containing the word "bribe;"

   c. Any communication, written or electronic, between KERN, the HUNTING CONSORTIUM, and any affiliated individuals about the payments of bribes to facilitate hunting trips; and

   d. Any business records related to the acquisition, taking, purchase, sale, booking, packaging, storage, or distribution of wildlife guide or booking services, wildlife or wildlife parts, including but not limited to ledgers, canceled checks, receipts, shipping documents, price lists, invoices, customer and service lists, quality control records, log books, journals, facsimile letters, notes, address books, advertising flyers and catalogues, diaries, correspondence, photographs, videotapes, DVDs, emails, permits, licenses, telephone records, airway bills, inventories, and wire transfer records related to trips where a bribe was paid to facilitate hunting trips.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

5. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or

storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

6. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.